



พ.ศ. ๒๕๖๗/๑ ๗๖

สำนักงานสาธารณสุขอำเภอชุมแพ

ตำบลสี อำเภอชุมแพ

จังหวัดศรีสะเกษ ๓๐๑๕๐

๑๙ พฤษภาคม ๒๕๖๗

เรื่อง ขอให้พัฒนาบ้านป้อมกัน ติดตาม เผ้าขาวด้วยส่วนราชการมีภารกิจความทางที่ชอบจริง

เรียน ผู้อานวยการโรงพยาบาลส่งเสริมสุขภาพตำบลทุกแห่ง

วันที่สี่สิบห้าปี สามสิบห้าชั่วโมงที่สี่สิบห้าวันเดือนเมษายน พ.ศ. ๒๕๖๗ ๑๔๐๘๖๔
ลงวันที่ ๒๘ พฤษภาคม ๒๕๖๗

จำนวน ๑ ชุด

ด้วยสำนักงานสาธารณสุขอำเภอชุมแพ ได้รับแจ้งจากสำนักงานสาธารณสุขจังหวัดศรีสะเกษ ศูนย์บริการจัดการธุรกิจท้องถิ่นและศูนย์ป้องกันควบคุมโรคเชเบอร์ (Health CERT) แจ้งผลการสำรวจภาวะโภชนาญาติกรดหรือสูตร สาธารณสุข เพื่อตรวจสอบติดตาม และเตรียมความพร้อมตอบสนองต่อเหตุการณ์ภัยคุกคามทางเชเบอร์ นี้

ในการนี้ สำนักงานสาธารณสุขอำเภอชุมแพ จึงขอความร่วมมือผู้รับผิดชอบพื้นที่ตามและเพื่อ ระวัง อย่างต่อเนื่อง ตามรายละเอียดตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อทราบและดำเนินการต่อไป

ขอแสดงความนับถือ

(นายสมัย คำเนก็อ)

สาธารณสุขอำเภอชุมแพ

สำนักงานสาธารณสุขอำเภอชุมแพ
โทร. ๐๕๕-๖๖๕-๒๓๒



ที่ ๓๙ ๑๗๗๗/ว ๗๖๐

สำนักงานสาธารณสุขอำเภอชุมทาง

สำนักงานชุมทาง

จังหวัดศรีสะเกษ ๓๓๑๕๐

๑๖ พฤศจิกายน ๒๕๖๖

เรื่อง ขอให้พนักงานป้องกัน ดูแลความ เฝ้าระวังสถานการณ์ภัยคุกคามทางเชื้อเบอร์

เรียน ผู้อำนวยการโรงพยาบาลส่งเสริมสุขภาพตำบลทุกแห่ง

เรื่อง ให้พนักงานป้องกัน ดูแลความ เฝ้าระวังสถานการณ์ภัยคุกคามทางเชื้อเบอร์

ลงวันที่ ๒๘ ตุลาคม ๒๕๖๖

สำนักงานชุมทาง

ด้วยสำนักงานสาธารณสุขอำเภอชุมทาง ได้รับแจ้งจากสำนักงานสาธารณสุขจังหวัดศรีสะเกซ ศูนย์บริการด้านการดูแลความปลอดภัยเชื้อเบอร์ (Health CERT) แจ้งพัฒนาภัยได้แก่เชื้อไวรัสโคโรนา สายพันธุ์ ๓๖๑๔ ที่ได้ระบาดในประเทศไทย ล่าสุดพบผู้ติดเชื้อรายแรกในประเทศไทย เมื่อวันที่ ๒๘ ตุลาคม ๒๕๖๖ คาดว่าเชื้อไวรัสโคโรนาสายพันธุ์ ๓๖๑๔ จะระบาดในประเทศไทยต่อไป ดังนั้น

ในการนี้ สำนักงานสาธารณสุขอำเภอชุมทาง จึงขอความร่วมมือผู้รับผิดชอบพัฒนาภัยไว้ ระวัง อย่างต่อเนื่อง ตามรายละเอียดตามลิสต์ที่ส่งมาด้วย

จึงเรียนมาเพื่อทราบและดำเนินการต่อไป

ขอแสดงความนับถือ

(นายสมัย คำเหลือง)

สาธารณสุขอำเภอชุมทาง

สำนักงานชุมทาง

โทร. ๐๔๔-๖๖๙-๒๓๒



สำนักงานสาธารณสุขอำเภอพุนหาย
วันที่ ๓๖๕๓ /๒๕๖๖
วันที่ ๙ ก.ย. ๒๕๖๖
เวลา ๑๕.๐๑.๖๖

ที่ ศก ๑๓๗๗/๔ ๗๗๗

ถึง อร่ามเกอทุก่อ เกอ โรงพยาบาลศรีสะเกษ โรงพยาบาลกันทรลักษ์ และโรงพยาบาลพุนพิน ทุกแห่ง

พัฒนาชีวิตคุณภาพ ขยายตัวในหนังสือสำนักงานปลัดกระทรวงสาธารณสุข ด่วนที่สุด
ที่ สธ.๑๒๑๒/ว๒๗๗๗ ลงวันที่ ๒๙ ตุลาคม ๒๕๖๖ เรื่อง ขอให้หน่วยงานป้องกัน ติดตาม เฝ้าระวัง
สถานการณ์ภัยคุกคามไว้เช่นเดิม สามารถติดตามรายละเอียดได้ที่ (เข้าชมเว็บไซต์) www.ssko.moph.go.th

จึงเรียนมาเพื่อโปรดทราบและดำเนินการต่อไปด้วย

เรียน นายอ่ำเกอพุนพิน¹
เพื่อโปรดทราบ

นายอ่ำเกอพุนพิน¹
นายพิษัย วงศ์งาม
นายอ่ำเกอพุนพิน¹



นายพิษัย วงศ์งาม
นายอ่ำเกอพุนพิน

(นายกานกร อุ่นคำ)

สำนักงานสาธารณสุขจังหวัดศรีสะเกษ การสาธารณสุขชำนาญการ
ศูนย์เทคโนโลยีสารสนเทศ
โทร ๐-๔๔๒๑-๖๐๔๐-๖ ต่อ ๓๑๘
โทรสาร ๐-๔๔๒๑-๖๐๔๒

ทราบ

พิษัย

(นายสมัย คำเหลือ)

สำนักงานสาธารณสุขอำเภอพุนพิน

อุ่น
กานกร

สำนักงานศุลกากรสุขจังหวัดเชียงใหม่
ชั้นที่ ๔๙๙๑/๒
วันที่ ๒๗ กุมภาพันธ์ ๒๕๖๓
เวลา ๐๘.๓๐



ความเห็น

ที่ สธ ๐๒๑๒/๒ ๒๗/๒๕๖๓

สำนักงานปลัดกระทรวงสาธารณสุข
ถนนพิริยาณนา แขวงหัวดันนทบุรี ๑๑๐๐๐

๒๗ กุมภาพันธ์ ๒๕๖๓

ลงนามในเอกสารนี้แล้ว
วันที่ ๒๗ กุมภาพันธ์ ๒๕๖๓
๒๗ กุมภาพันธ์ ๒๕๖๓

เรื่อง ขอให้หน่วยงานป้องกัน ติดต่อ สำรวจสถานการณ์ภัยคุกคามทางไซเบอร์

เรียน เอกอัครราชทูตกระทรวงสาธารณสุข/อดีตกรรมทูต/นายแพทย์สาธารณสุขจังหวัดเชียงใหม่/ อ.๑๐

ผู้อำนวยการสำนักงานเขตทุ่งพญาไท ๑ - ๗๙๙๑ ผู้อำนวยการโรงพยาบาลศุภชัย/ท่าไป/ท่าหน้า
สำนักงานรัฐวิสาหกิจ และผู้อำนวยการหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

สิ่งที่ต้องมาด้วย เอกสารการพัฒนาบินการเพื่อตรวจสอบการณ์ภัยคุกคามทางไซเบอร์

เข้าร่วม ๑ ฉบับ

ด้วยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ในฐานศูนย์ประสานการรักษาความมั่นคง
ปลอดภัยไซเบอร์ (Health CERT) ได้รับแจ้งเตือนจากสำนักงานคณะกรรมการการวิชาชีววิทยาฯ ของประเทศไทย
ไซเบอร์แห่งชาติ (ศกนช.) พบความคืบหน้าในเว็บไซต์ Hackthissite อ้างถึงเหตุการณ์สังหารไม่ชอบธรรมอย่างกว้าง
โดยกำหนดเป้าหมายการโจมตีทางไซเบอร์ที่หน่วยงานภาครัฐของประเทศไทย เมื่อวันที่ ๒๖ ตุลาคม ๒๕๖๒

Health CERT พิจารณาแล้วเห็นว่าเป็นเรื่องจริงตามที่อธิบายไว้ จึงขอแจ้งให้อ่านหน่วยงานภายในภายใต้สังกัด
กระทรวงสาธารณสุขทราบเช่นเดียวกัน เพื่อตรวจสอบพัฒนาและเตรียมความพร้อมเพื่อตอบสนองเหตุการณ์
ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ทั้งนี้ Health CERT ได้เฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์รวมกับ
หน่วยงานภายในได้ตั้งแต่วันที่ ๒๖ ตุลาคม ๒๕๖๒ จนถึงวันที่ ๒๗ ตุลาคม ๒๕๖๒
พบเหตุการณ์ที่อาจเกิดขึ้นกับการถูกโจมตีชั่วขณะ ๓ เหตุการณ์ ซึ่งเป็นการโจมตีหน้าบ้านไปสู่ที่อยู่อาศัย
โดยผ่านระบบเครือข่าย ("Gophersite") โดยเป็นไปทั้งตั้งเดียวหรือเป็นกลุ่ม (HTTP)
และได้ดำเนินการต่อสนองเบื้องต้นแล้ว ทั้งนี้ ยังไม่พบเหตุการณ์ข้อมูลรั่วไหล หรือกรณีวิกฤตที่มีผลกระทบ
ต่อการให้บริการ

ดังนั้น เพื่อให้หน่วยงานภายในได้รับภัยคุกคามทางไซเบอร์ป้องกัน ที่ด้วยความระมัดระวัง
ลดการณ์ภัยคุกคามทางไซเบอร์ดังกล่าวอย่างต่อเนื่องและตรวจสอบ จึงเห็นควรที่จะดำเนินการเเจ้งอย่างเป็นทางการ
พร้อมข้อแนะนำในการดำเนินการเฝ้าระวังเหตุการณ์ภัยคุกคามทางไซเบอร์ รายละเอียดตามสิ่งที่ต่อไปนี้

จึงเรียนมาเพื่อโปรดทราบและแจ้งผู้ที่มีอำนาจให้ทราบโดยทันที พร้อมทั้งดำเนินการในส่วน
ที่เกี่ยวข้องอย่างเคร่งครัดต่อไปด้วย

ผู้ช่วยศาสตราจารย์ ดร. นพ. พันธุ์ ใจดี

ขอแสดงความนับถือ

นายพันธุ์ ใจดี
ผู้ช่วยศาสตราจารย์ ดร. นพ. พันธุ์ ใจดี
ผู้ช่วยศาสตราจารย์ ดร. นพ. พันธุ์ ใจดี

(นายพันธุ์ ใจดี)

ผู้ช่วยศาสตราจารย์ ดร. นพ. พันธุ์ ใจดี

ศูนย์ป้องกันการวิชาชีววิทยาและแพทย์แผนไทยเชียงใหม่ จังหวัดเชียงใหม่

สำนักงานสาธารณสุข (Health-CERT)

ปฏิบัติงานการเเจ้งให้ทราบโดยทันที

(นายพันธุ์ ใจดี)

โทร. ๐ ๖๖๕๘ ๑๒๐๐, ๑๕ ๑๖๙๔ ๔๔๙๘

นายนพดล ใจดี (ผู้ช่วยศาสตราจารย์ ดร. นพ. พันธุ์ ใจดี)
นายนพดล ใจดี (ผู้ช่วยศาสตราจารย์ ดร. นพ. พันธุ์ ใจดี)

โทร. ๐ ๖๖๕๘ ๑๒๐๐, ๑๕ ๑๖๙๔

นายนพดล ใจดี (ผู้ช่วยศาสตราจารย์ ดร. นพ. พันธุ์ ใจดี)



การดำเนินการเฝ้าระวังสอดส่องตรวจสอบความปลอดภัยของระบบเครือข่าย

จากการแจ้งเตือนให้เห็นชัดเจนเฝ้าระวังการโจมตีของกลุ่ม hacker โดยอ้างเหตุการณ์ส่งผลกระทบในด้านอุตสาหกรรม ได้ยังเป้าหมายที่หน่วยงานภาครัฐของประเทศไทยนั้น เพื่อเป็นการยกระดับการเฝ้าระวังและป้องกันการโจมตีดังกล่าว ควรดำเนินการเฝ้าระวังสถานการณ์คุกคามทางไซเบอร์ดังนี้

1. หากตรวจสอบพบ IP Address ต่างประเทศ หรือไม่ระบุตัวตน แปลง ๆ เป็นพยายามทำการ Login (Brute-force) หรือพฤติกรรมอื่น ๆ ที่ไม่เป็นมาตรฐานในการเข้าสู่ระบบ เช่น การบุกเบิกหรือการซ่อนตัวไว้เพื่อหลอกลวงให้คนภายนอก
2. ตรวจสอบ Log Firewall, Server เพื่อเฝ้าระวังการเข้าถึงจากภายนอก ระบบเครือข่าย รวมถึงการเข้ามายังเครื่อง Server และมีการรับข้อมูลบุก入
3. ตรวจสอบ Policy ของ Firewall ว่ามีการกำหนดได้อย่างถูกต้อง ครบถ้วน และครอบคลุมการเข้าถึง Service Port ของเครื่องคอมพิวเตอร์ที่อาจถูกโจมตี ระบบเครือข่าย (Port) ที่สำคัญ และไฟแอลฟ์ที่ต้องใช้ ฐานข้อมูล ได้มาจากเครือข่ายอินเทอร์เน็ต
4. ตรวจสอบการเข้าใช้งาน Remote Desktop จาก IP ต่างประเทศป้อนยศรหัส พนักงานที่มีการนำ Credentials ที่ถูกโอนไปบ้านมาใช้งาน
5. หากพบการโจมตีเกิดขึ้นทันทีโดยชัดเจน ควรตัดการเชื่อมโยงเครือข่ายออก จากระบบเป็นการชั่วคราวและแจ้งเหตุการณ์ให้แก่ Health CERT (@health-cirt) ทราบโดยด่วน เพื่อจะได้ประสานและดำเนินการในลักษณะ เกี่ยวกับข้อต่อไป
6. ให้ดำเนินการตามนโยบาย แนวปฏิบัติ และมาตรการการรักษาความมั่นคง ปลอดภัยไซเบอร์ ตามที่ได้มีการแจ้งไว้ยอมรับอย่างหน่วยงานในสังกัด กระทรวงสาธารณสุขไปแล้วนั้น อย่างต่อเนื่องและเคร่งครัดต่อไป

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์
ด้านสาธารณสุข (Health-CERT)
โทรศัพท์ 08 3064 9867, 0 2590 1201
อีเมล: health-cirt@moph.go.th
Line Official: @health-cirt

